



The Technology Optimist's View on Product Security

Matthias Luft

matthias.luft@rational-security.io

aws sts get-caller-identity

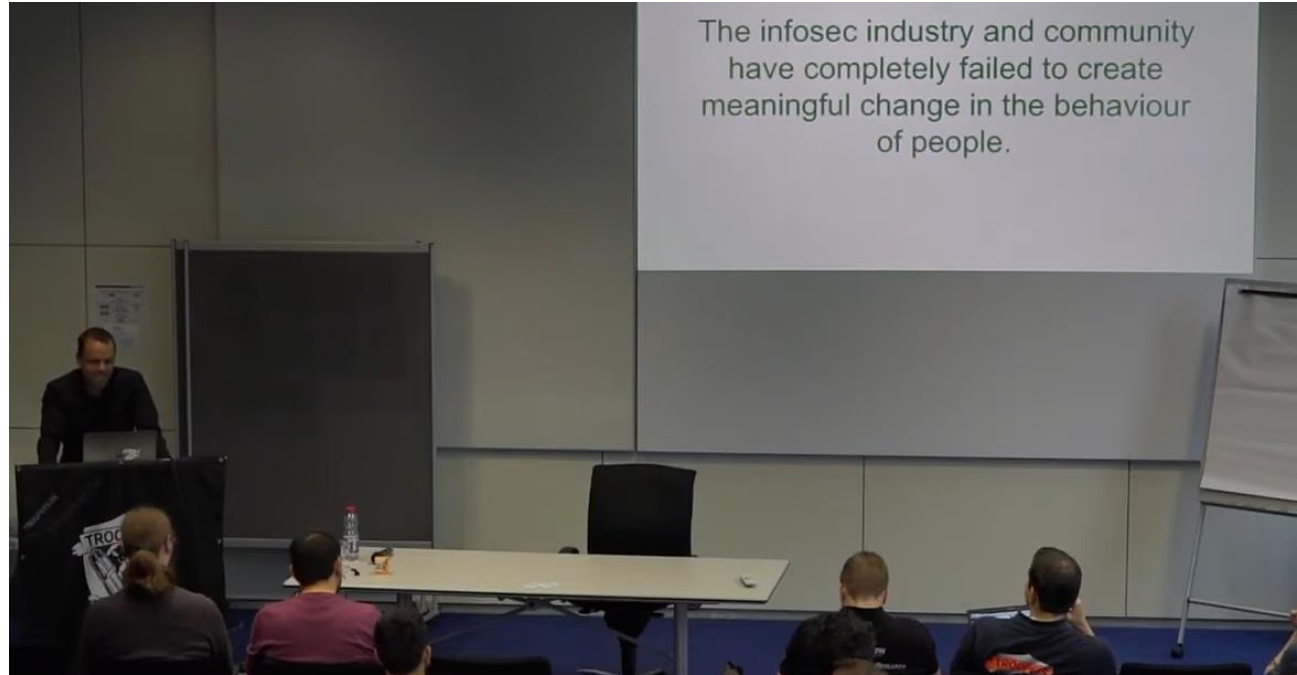
- Matthias Luft
- Principal Security Researcher @ Averlon
- Pentesting ->
Security Research ->
Leadership ->
Security Engineering ->
Security Research



Why this talk?



Evil Imp's Manifesto in 2018





Privilege of In-Person Discussion of this talk about 7 years later

... and me being an optimist and having worked in some amazing engineering orgs.

My Background

- Cloud-native environments
- Very different from:
 - OT
 - Old, overgrown environments
 - Endpoints 🤖



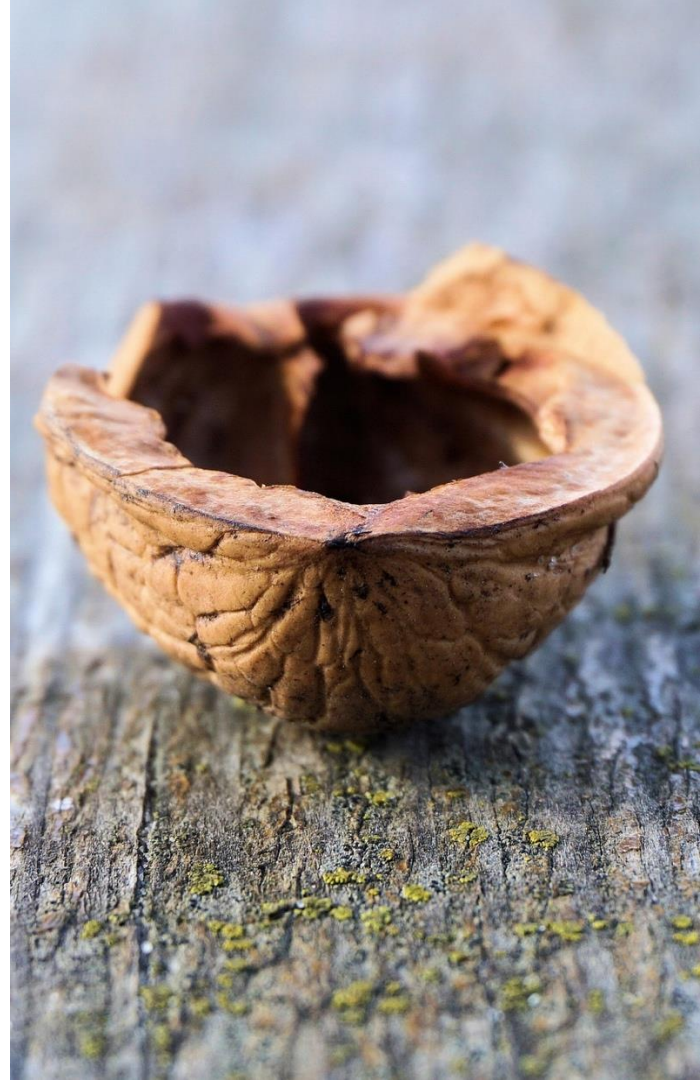
My Background

- Cloud-native environments
- Very different from:
 - OT
 - Old, overgrown environments
 - Endpoints 🤖
- Very different... so far!
 - The things I will be talking about can be adopted to any field.



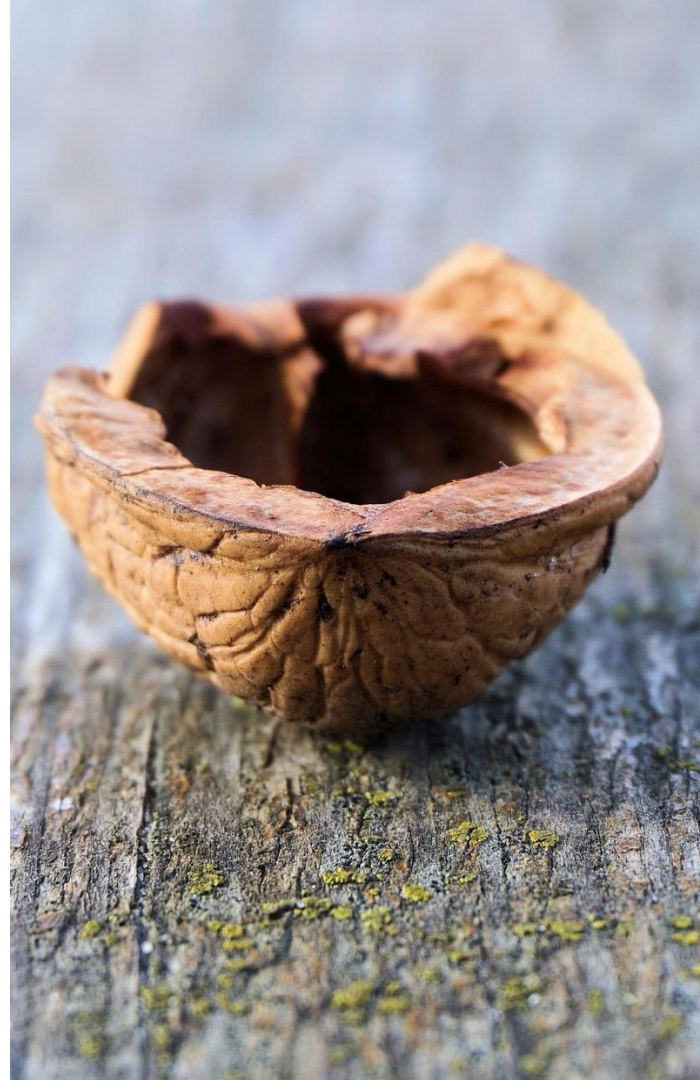
Evil Imp's Manifesto

- Untrusted Input has been a huge problem for a long time
- Nothing changed
- Artistic disclosure



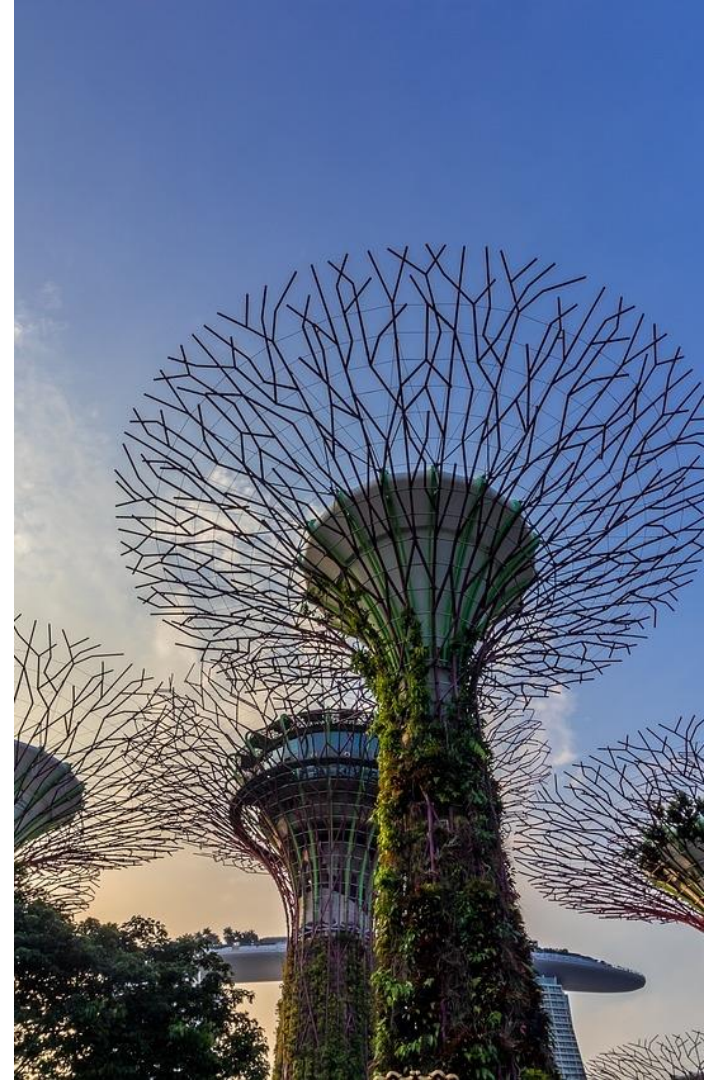
Evil Imp's Manifesto

- Untrusted Input has been a huge problem for a long time
- **Nothing changed**
- Artistic disclosure

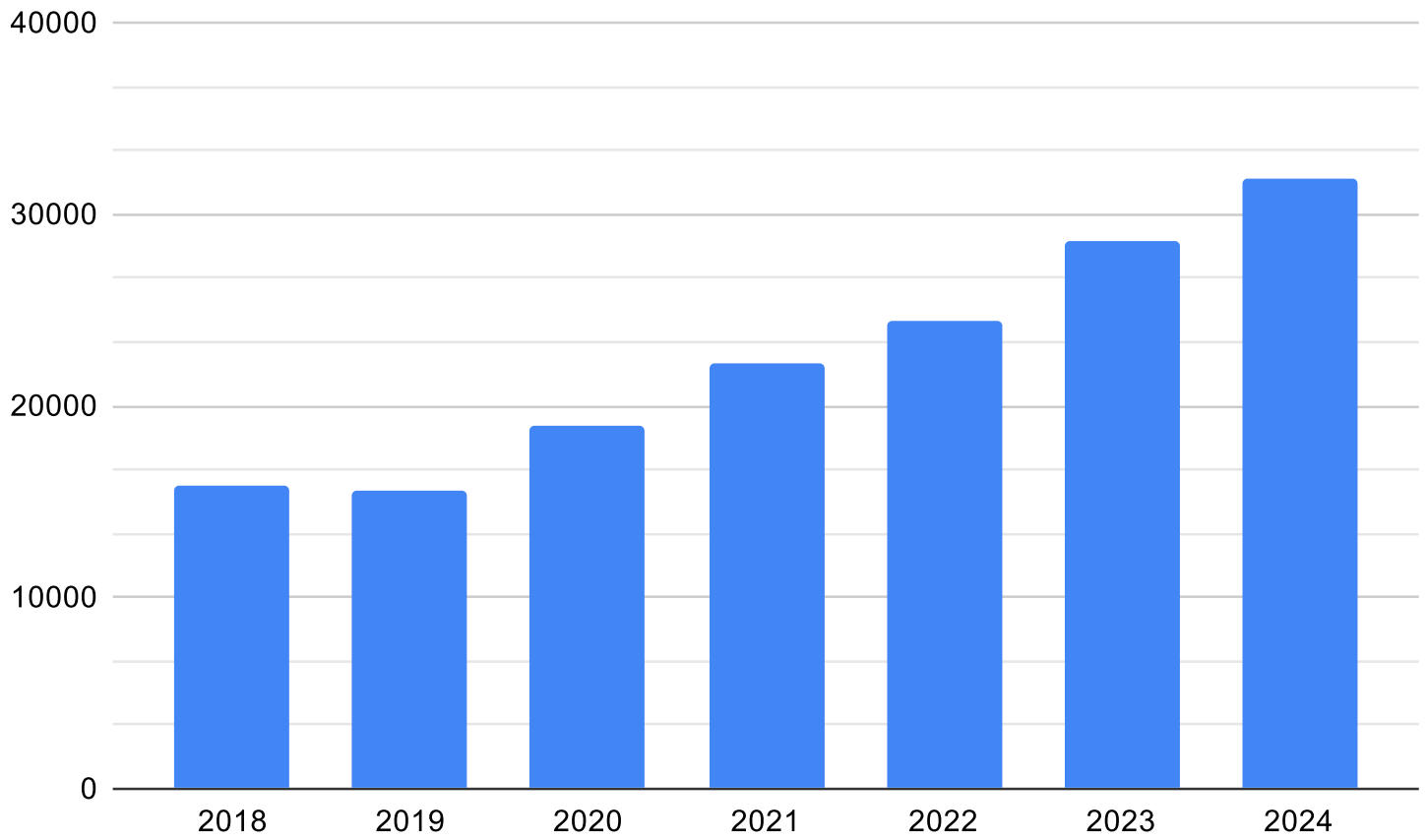


Technology Optimism

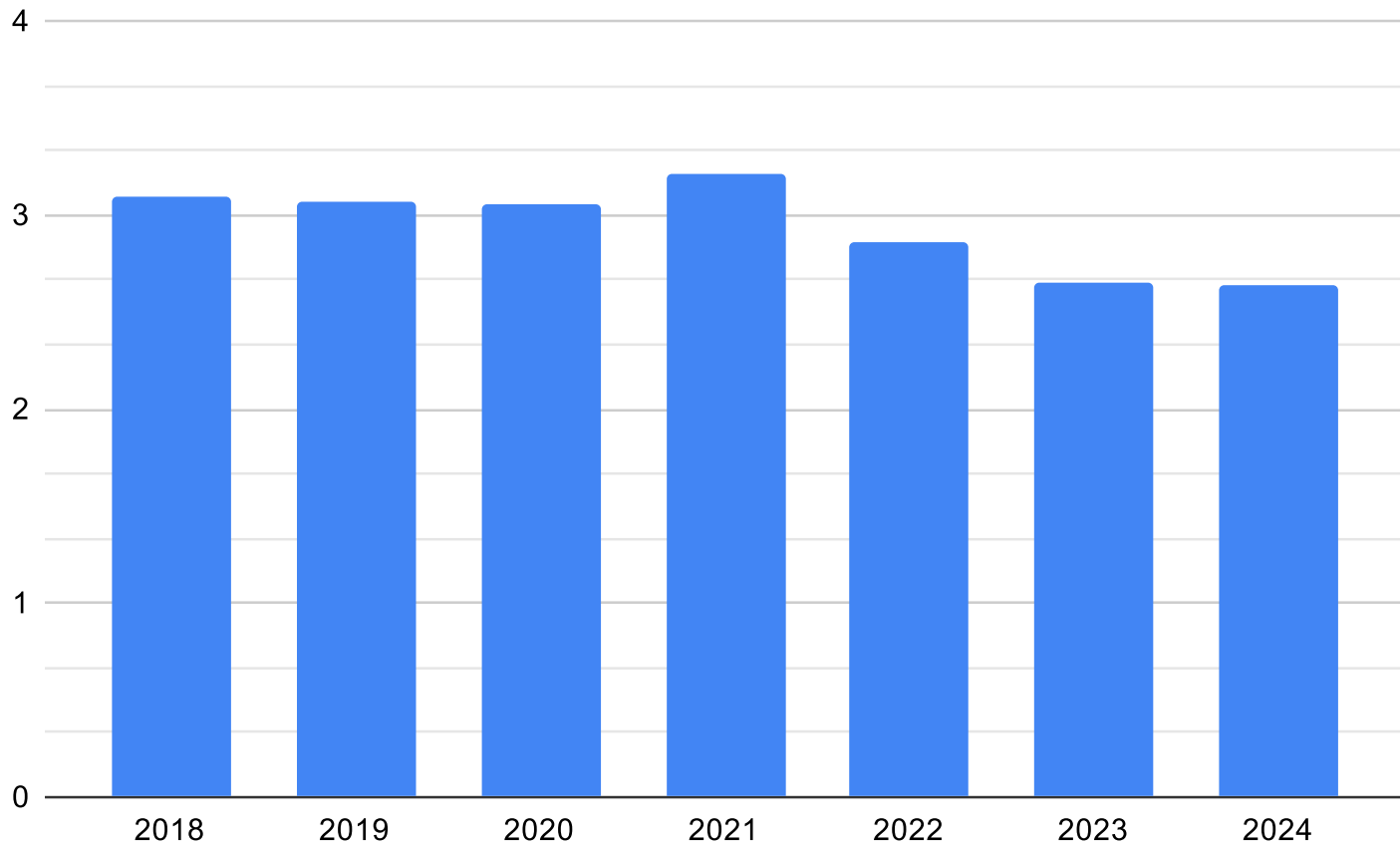
- I am optimistic about technology and technology gives me optimism
 - I heard the term first on this [\(recommended\) substack](#)
- The term itself can send you down a rabbit hole though and I did not go down deep enough to endorse/distance myself from a lot of it:
 - <https://a16z.com/the-techno-optimist-manifesto/>
 - Opposed by 'Techno-optimism is a dangerous philosophy whose adherents espouse the blind faith that market capitalism and technology will solve the world's problems. In reality, this kind of optimism simply justifies elite power and promotes indifference to human suffering.' (2023)
 - [Peter Königs - What is Techno-Optimism? \(2022\)](#)
 - [The Un-Easy Case for Technological Optimism \(1985\)](#)
 - [UN Has a take as well](#)



CVEs per Year

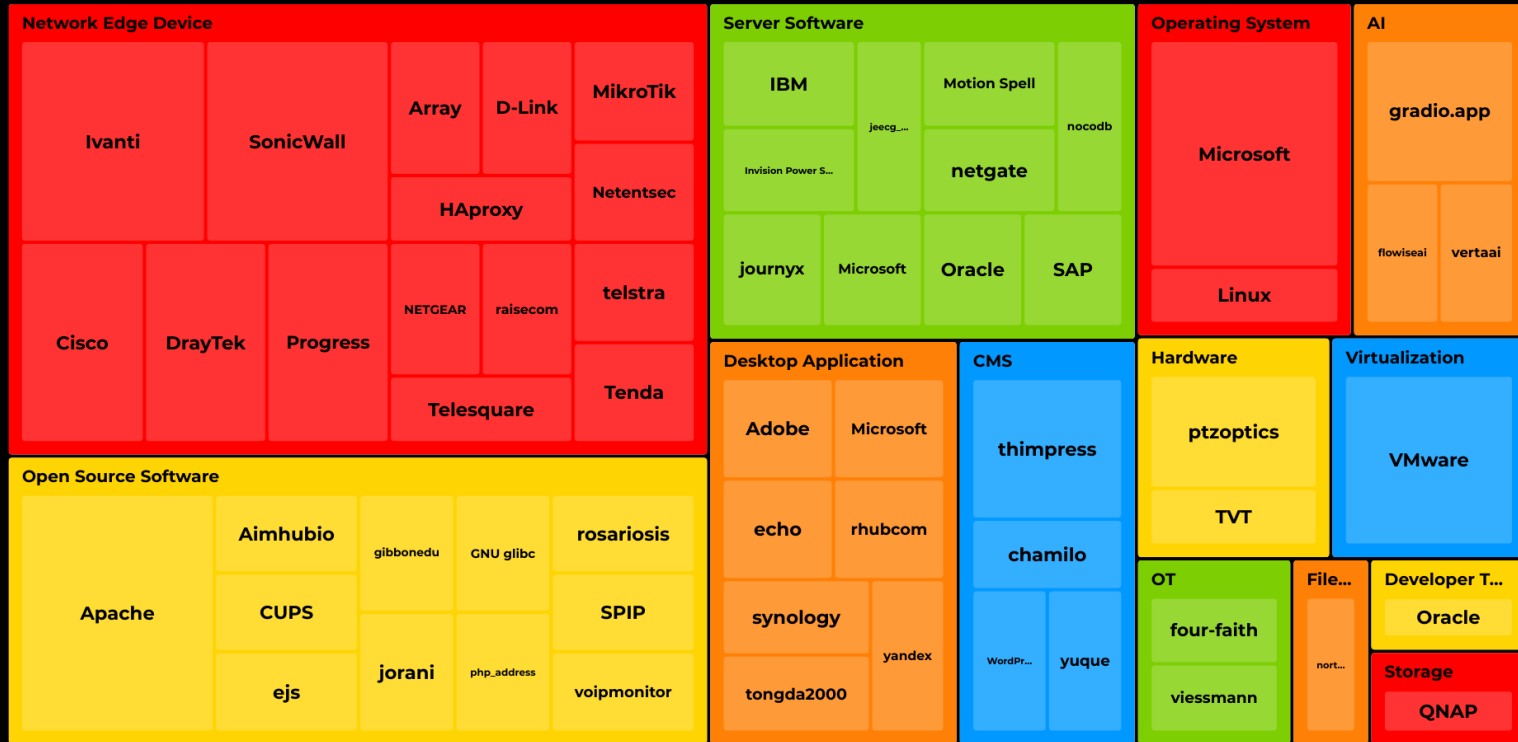


CVEs per Product



VulnCheck Known Exploited Vulnerabilities

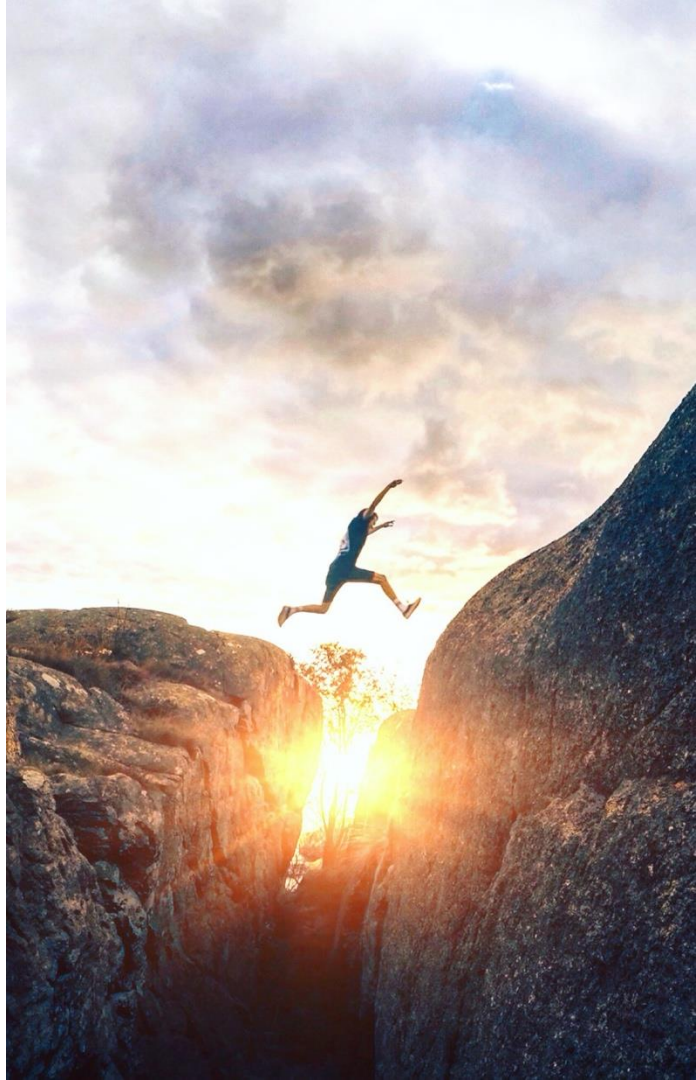
(Reported September - 2024)



Known Exploited Vulnerabilities
Source: [Vulncheck](#)

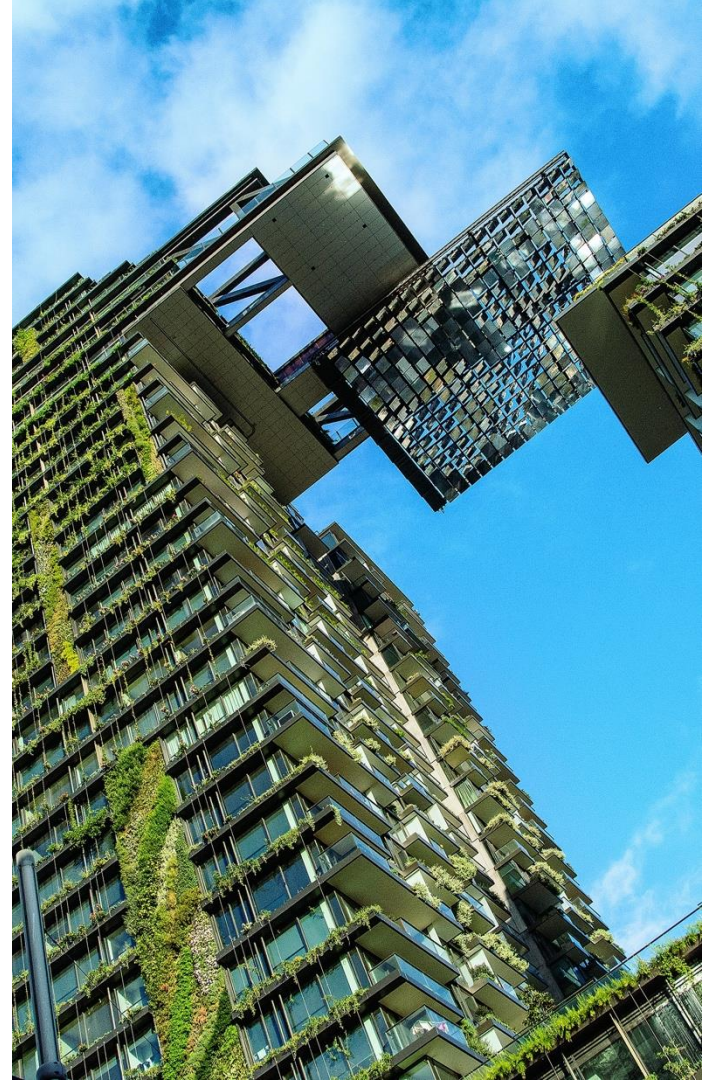
Hacker to Optimist

- I hated Software Engineering in University
 - Anybody remember Java Enterprise Stacks?
- Along came Docker and DevOps
- Software structure aligned more with infrastructure
- Software, in my personal experience, became way easier to manage and more stable



Modern Engineering Organizations

- Relevance of security was never debated
- Focus on advancing the product



Keep Security Non-negotiable

- With great power comes great responsibility.
- Understand that security must be an enabler.
- Focus on the important.

- Many additional talks could and are filled with the above.



Vulnerability Management

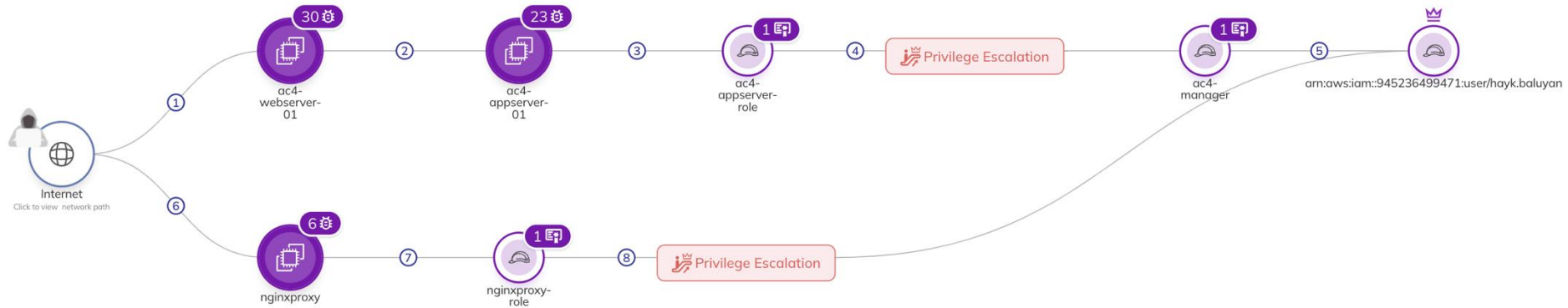
- No relevant application-level vulnerability besides Log4J in 3 years of triaging for a large code base.
 - Exception: Compromised packages
- Do a regular update schedule and forget about it.
- Mandatory talk recommendation:
[When data contradicts security best practices | Stripe Sessions 2019](#)



Cloud

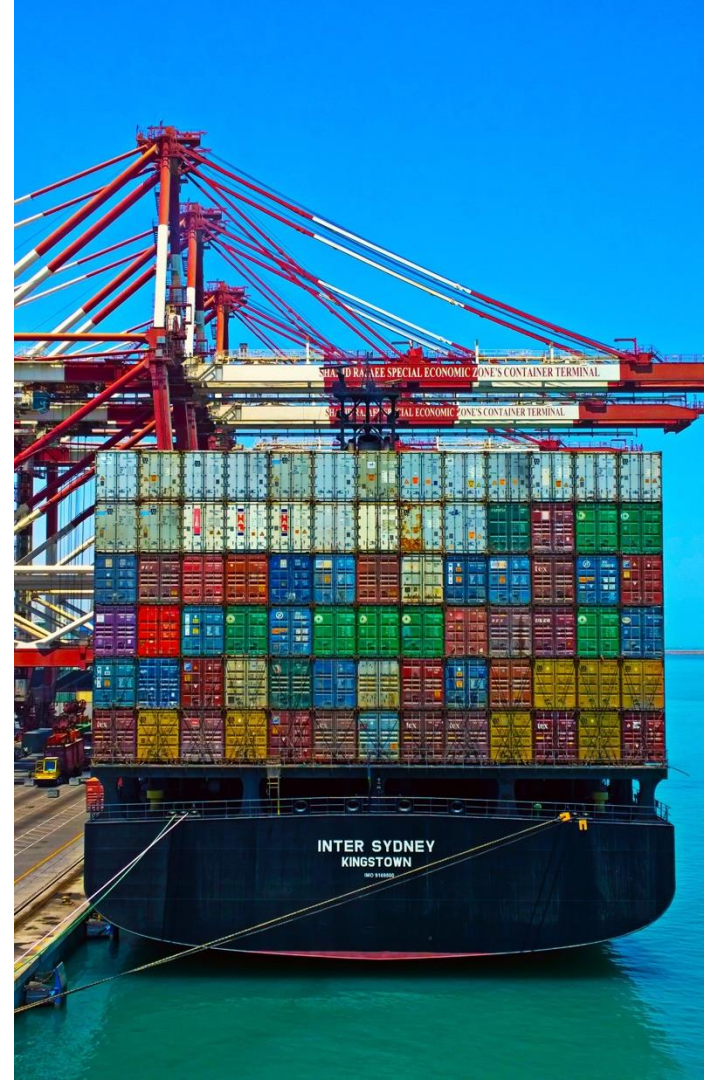
- Orchestrate and automate everything
- Leverage Drift Control






Containers

- Decouple application from infrastructure
 - Minimal runtime environments
 - Sandboxing
 - Essential for short update intervals
-
- BTW: Made a big appearance in the embedded world.



The full picture

- Cloud
- IaC
- CI/CD
- Driftctl
- Update schedule
-  takes care of the busywork so you can focus on the hard problems with your application.




Bazaar coming to life?

- I am still amazed that the xz backdoor was discovered.
- The level of maturity and security for many popular projects is fantastic to work with.
- We are legion
 - Even though we all miss the old days when we knew everyone, right? ;)

The bored guy who wanted to figure out why SSH was slower than .01ms? Hero, but Accidental her...

Hm, if you look at this one instance, maybe. However, our profession is full of people that just love to dig fully into those 0.1ms delay because that is what we do. Exactly the stuff Et digs up in assessments.

More importantly, if you change the viewpoint to this type of attacker, you need to take into account that infosec is full of people like that and factor that in. And thinking about it this way is amazing for infosec as a whole 

9:25 AM 

Obvious Issues with my Utopia

- Vulnerabilities in Cloud Services
- Supply Chain Security
- Privacy Challenges
- Complexity



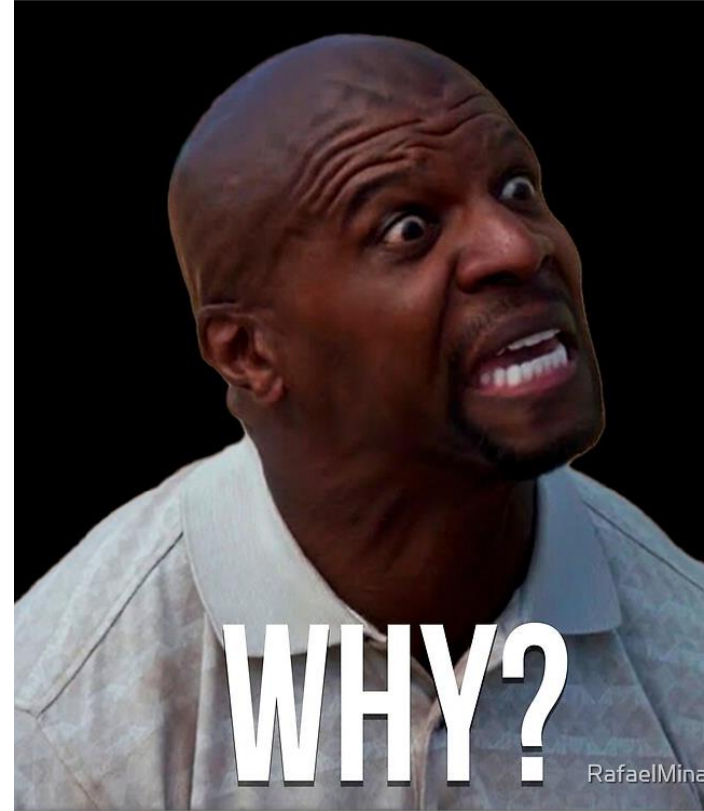
HOWEVER

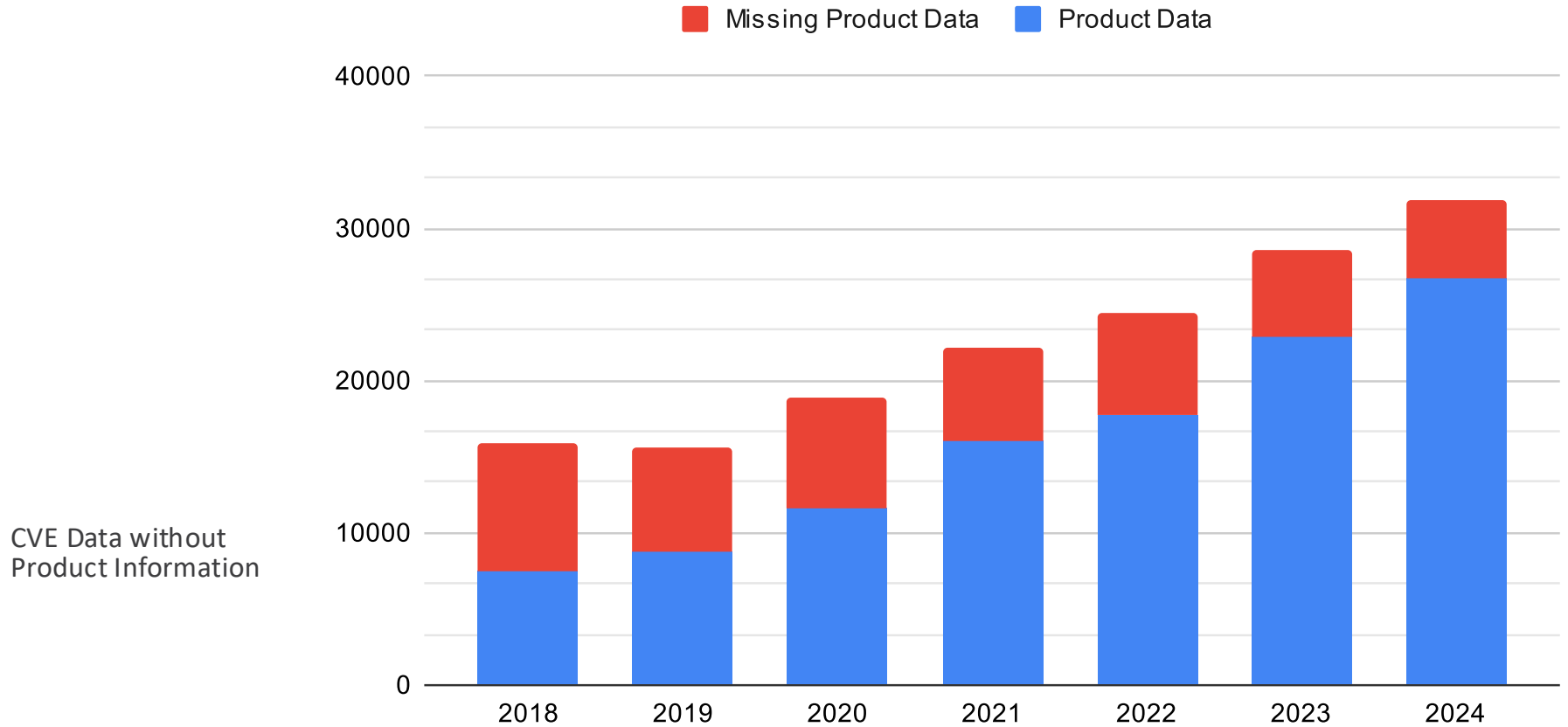
- Graeme making fun of 'don't click on links' deeply resonates with me.



Whyyyyyyyy?

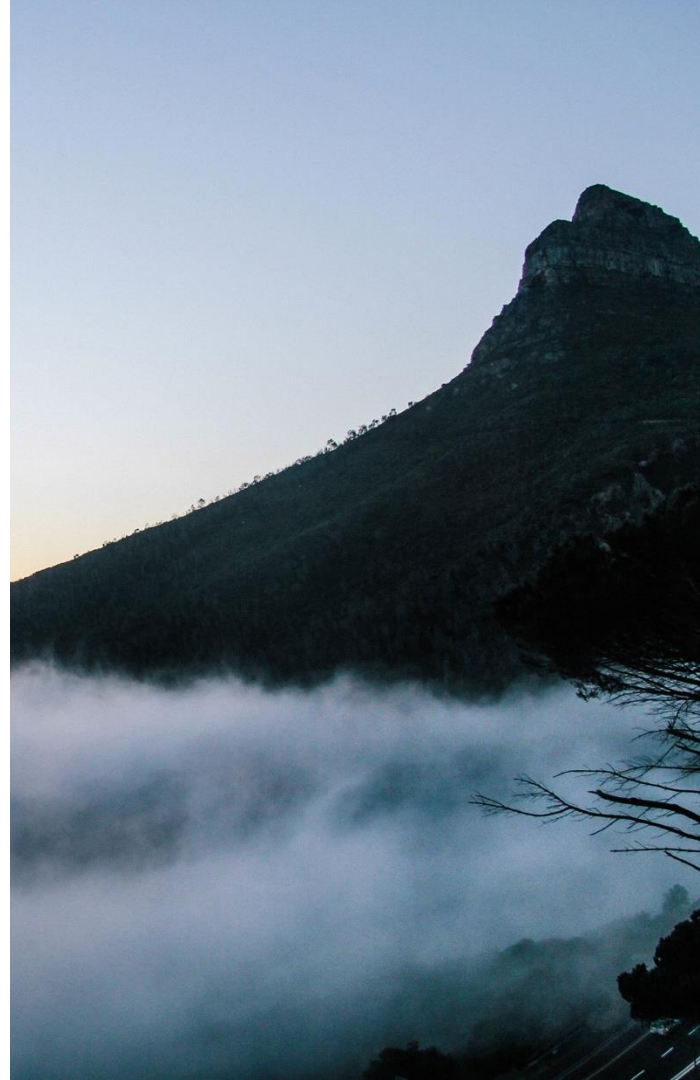
- How is basic BS about the CISO role still top content on LinkedIn?
- How did nobody think that different Apache Modules might be assuming different things before 2024?
- How did nobody realize default AWS resources are predictable and accessible?
- How did nobody ever try to have a browser access 0.0.0.0 before?
- How did nobody ever use a certain DHCP option for local network highjacking until 2024?





Conclusions

- Modern software can be built to a high security standard with reasonable effort.
- Modern infrastructure can be built and operated to a high security standard with reasonable effort.
- Still so many low hanging fruits out there!
- But you are less likely to include them in your product if you use modern ecosystems!



Thank you for your Attention!

... and see you for my next edgy talks

Abolish CISOs

and

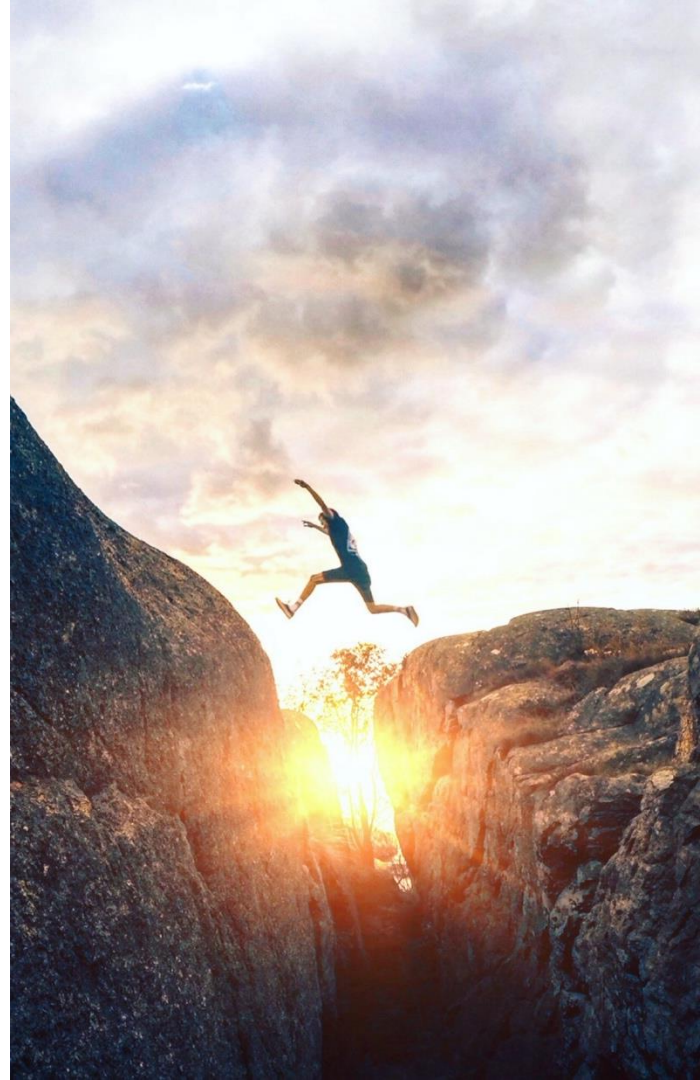
Nobody at DefCon will hack your burner



matthias.luft@rational-security.io



[@uchi_mata](#)



Appendix

- CVE Data Analysis
 - <https://github.com/CVEProject/cvelistV5>
 - <https://github.com/uchi-mata/cve-analysis>

